



How to Read a Privacy Policy

CONSUMER INFORMATION SHEET 6

One way to protect your privacy is to learn how an organization will use your personal information *before* you give it out. Today most financial institutions, insurance companies, government agencies, and many popular e-commerce Web sites give their customers some information on their privacy practices.¹ Before you fill out an application for credit or type your credit card number into an online order form, ask to see a copy of the organization's privacy policy. If you are not happy with the policy's terms—or if you are told there is no written privacy policy—STOP. Consider looking for another company that respects its customers enough to protect their personal information and to explain its privacy practices.

A privacy policy should answer at least these basic questions.

❑ WHAT personal information is collected?

Personal information that businesses and government agencies ask you for may include the following:

- your name and home address,
- your home phone number,
- your email address,
- your Social Security number and your driver's license number,
- your financial information, such as credit card numbers, bank account numbers, and household income,
- your medical information, such as your health insurance plan, diseases or physical conditions, and prescription drugs used,
- your education and work experience, and
- other details of your personal life, such as your date of birth, the names and ages of your spouse or children, and your hobbies.

❑ WHY is the information collected?

Is the personal information asked for appropriate to the transaction? For example, your name, home address, phone number, and credit card number may be necessary for making and shipping your purchase. Your household income and hobbies are not. Pay attention if a business or web site asks for information beyond what is needed for



the transaction. The purpose for the extra information should be clearly stated. Look for an opportunity to opt out of giving the extra information.

❑ **HOW is the information used?**

A privacy policy should explain how the organization collecting the personal information intends to use it. Will it be used just to complete the transaction you requested? If additional uses are intended, you should be given the opportunity to opt out. For example, if a merchant plans to use your information to market to you, you should be given an easy way to say no to this. You should get this opportunity right up front, before you receive any unwanted email ads or telemarketing calls.

❑ **WHO will have access to the information?**

Does the company or Web site share customer information with other companies? Does it share information with its affiliates or companies in the same “corporate family”?

❑ **WHAT CHOICES do you have?**

Look for opportunities to opt out of, or say no to, the use of your information for marketing and the sharing of your information with other companies. There should be an easy way to opt out, such as calling a toll-free phone number or sending an email.

The Center for Democracy and Technology has created [Operation Opt-Out](#) to help you get off mailing and telemarketing lists and limit the sharing or sale of your personal information.² Their Web site contains forms you can print out and mail or send online to opt out of information sharing by Web portals, data aggregators, and many businesses.

According to *Consumer Reports’* E-Ratings, the better companies and Web sites do not share personal customer information with other unrelated companies unless the customer consents in advance.³

❑ **WHAT SECURITY measures are used to protect your personal information?**

The policy should describe the security measures the organization uses to keep customers’ personal information safe.

Web sites requesting personal information should use Secure Socket Layers (SSL), the industry standard in transferring information to process your orders. Your order information is encrypted, or scrambled, into a code as it is sent over the Internet. This means that your information can’t be intercepted in transmission. Look for signs of



security on Web pages where you enter personal information. Look for “https,” rather than the usual “http,” in the address window. Look for a closed lock icon in the lower right or left corner of your screen. These signs means the connection is secure. You should remain in this secure zone for the entire checkout process.

Good security also means using strong security, such as encryption, to protect personal information when it’s stored on company computers. It includes limiting access to customers’ personal information to those who need it to perform their duties.

❑ **HOW LONG will the organization honor its privacy policy?**

Does the policy state that the organization will honor its current policy in the future? Does it say that if they do change the policy, they will notify customers? Does it say they will give customers a chance to opt out of having their information used according to the terms of the new policy?

❑ **WHO is accountable for the organization’s privacy practices?**

Someone in the organization should be responsible for its privacy policy and practices. Does the policy give you someone to contact with questions or concerns? Is there an easy way to contact the right person—by email or by a toll-free phone number?

Additional Questions for Web Site Privacy Policies

❑ **How is the information collected?**

Does the Web site set cookies? Internet cookies are small text files placed on your computer by a Web site you visit. A cookie contains information on you that your browser saves and sends back to a Web server when you visit it again. Cookies do not always pose privacy problems. Most are used simply to store a user ID on your machine in order to determine how many people visit. Cookies make online shopping convenient. Cookies can also enable marketing communications. A Web site can use cookies to track your purchases and also the different pages you visited or ads that you clicked on. That can create a richer profile on you that can be sold to marketers. For more information on cookies and how to manage them, see EPIC’s cookie page at www.epic.org/privacy/internet/cookies/.

❑ **Does the site have a privacy seal?**

TRUSTe and **BBBOnline** are voluntary programs that require Web sites that carry their “seal of approval” to agree to follow certain privacy practice guidelines.⁴ Both



programs require seal holders to give customers some choice on how their information will be used. Both programs also offer assistance with consumer complaints.

For More Information on Reading Privacy Policies

Center for Democracy and Technology, "Getting Started: Website Privacy Policies," at www.cdt.org/privacy/guide/start/privpolicy.html.

Privacy Rights Clearinghouse, "Financial Privacy: How to Read Your 'Opt-Out' Notices," at www.privacyrights.org/fs/fs24a-optout.htm.

Privacy Toolbox, "How to Read A Privacy Policy," at www.privacytoolbox.org/shopping/policy.shtml.

This fact sheet is for informational purposes and should not be construed as legal advice or as policy of the State of California. If you want advice on a particular case, you should consult an attorney or other expert. The fact sheet may be copied, if (1) the meaning of the copied text is not changed or misrepresented, (2) credit is given to the Office of Privacy Protection in the California Department of Consumer Affairs, and (3) all copies are distributed free of charge.

Notes

¹ The federal Financial Services Modernization Act requires financial institutions and insurance companies to send a privacy notice to customers every year. See the Financial Privacy page on the Office of Privacy Protection Web site at <http://www.privacy.ca.gov/financial.htm> for more information. The federal Health Insurance Portability and Accountability Act requires health care providers, health plans, and health insurers to provide patients with notice of the patient's privacy rights and the privacy practices of the covered entity. More information is available at <http://aspe.hhs.gov/admsimp/bannerps.htm#privacy> and at <http://www.healthprivacy.org/>.

² The Center for Democracy and Technology (CDT) is a non-profit policy organization that works to promote democratic values and constitutional liberties in the digital age. Their Web site is at www.cdt.org. Operation Opt-Out is at <http://opt-out.cdt.org/>.

³ See Consumer Reports, *E-Ratings: A Guide to Online Shopping, Services, and Information*, available at www.consumerreports.org/.

⁴ Information on TRUSTe's program can be found at www.truste.com/consumers/users_how.html and on BBBOnline's at www.bbbonline.com/privacy/.